

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

**DAVID CAPLAN, individually and on  
behalf of all others similarly situated,**

**Plaintiff,**

**vs.**

**EQUIFAX INFORMATION  
SERVICES, LLC,**

**Defendant.**

**COMPLAINT – CLASS ACTION**

**NO.**

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff DAVID CAPLAN (“Plaintiff”), by and through his counsel, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Equifax Information Services, LLC (“Equifax” or “Defendant”), alleging the following:

**PARTIES, JURISDICTION, AND VENUE**

1. Plaintiff DAVID CAPLAN is an adult individual residing in Montgomery County, Pennsylvania.

2. Plaintiff DAVID CAPLAN is, and at all times relevant was, a “consumer” as that term is understood under 15 U.S.C. § 1681a(c).

3. Defendant Equifax Information Services, LLC is a limited liability company incorporated under the laws of the State of Georgia with its principal place of business located at 1550 Peachtree Street NE, Atlanta, GA doing business in the Commonwealth of Pennsylvania.

4. Equifax is a “Consumer Reporting Agency” (or “CRA”) as that term is defined by 15 U.S.C. § 1681a(f).

5. Equifax is also a “Consumer Reporting Agency that Compiles and Maintains Files on Consumers on a Nationwide Basis” as that term is defined under 15 U.S.C. § 1681a(p).

6. This Court has jurisdiction over this matter pursuant to 28 U.S.C. § 1331, as this case alleges a violation of federal law, specifically the Fair Credit Reporting Act, 15 U.S.C. §§ 1681, *et seq.* (“FCRA”).

7. Venue in this District is proper pursuant to 28 U.S.C. §§ 1391(b) and (c), as the Plaintiff resides within this District, a substantial portion of the events or omissions giving rise to the claim occurred in this District, and Equifax regularly conducts business in this District.

### **INTRODUCTION**

8. The United States Congress has found the banking system to be dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods

undermine the public confidence, which is essential to the continued functioning of the banking system. Congress enacted the Fair Credit Reporting Act, 15 U.S.C. §§ 1681, *et seq.* (“FCRA”), to insure fair and accurate credit reporting, promote efficiency in the banking system, and, as most relevant to this Complaint, protect consumer privacy. The FCRA imposes duties on the CRA's to protect consumer's sensitive personal information.

9. The FCRA protects consumers through a tightly wound set of procedural protections from the material risk of harms that otherwise follow from the compromise of a consumer's sensitive personal information. Thus, through the FCRA, Congress struck a balance between the credit industry's desire to base credit decisions on accurate information, and a consumer's substantive right to protection from damage to reputation, shame, mortification, and emotional distress that naturally follows from the compromise of a person's identity.

10. A central duty that the FCRA imposes upon CRAs is the duty to protect the consumer's privacy by guarding against inappropriate disclosure to third parties. 15 U.S.C. § 1681b codifies this duty, and permits a CRA to disclose a consumer's information only for one of a handful of exclusively defined “permissible purposes.” To ensure compliance, CRAs must maintain reasonable procedures to ensure that such third party disclosures are made exclusively for permissible purposes. 15 U.S.C. § 1681e(a).

11. The FCRA defines “consumer report” broadly, as “any written, oral, or other communication of any information by a CRA bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title.” 15 U.S.C. § 1681a(d).

12. The FCRA also entitles the consumer to take an active role in the protection of his or her sensitive personal information, by giving the consumer a right to request “All information in the consumer’s file at the time of the request.” 15 U.S.C. § 1681g(a)(1). Through immediate review of the details of when, and for what purpose, a consumer’s information has been disclosed to a third party, a consumer may better understand whether their identity has been stolen.

13. The FCRA also entitles consumers to actively protect their privacy rights in cases of suspected identity theft. Specifically, a consumer who believes he or she has been the victim of identity theft can submit a fraud alert to a consumer reporting agency. 15 U.S.C. § 1681c-1. The consumer can either request that the fraud alert be imposed for a 90-day period, or for an extended period of seven years. 15 U.S.C. § 1681c-1(a)-(b). In the event a consumer requests “extended” protection,

a consumer reporting agency must remove the consumer from any list of third parties to whom the agency sends the consumer's information to extend firm offers of credit, and keep the consumer off of any such a list for five years, unless the consumer requests otherwise. 15 U.S.C. § 1681c-1(b)(1)(B). After being notified of a fraud alert, a CRA must send notification of the alert to the consumer reporting agencies which report information on a nationwide basis. 15 U.S.C. § 1681c-1(a)(1)(B); *see* 15 U.S.C. § 1681a(p).

14. After fraud notification, the FCRA provides the consumer additional rights to independently monitor their credit information to protect their privacy. Specifically, once notified of a consumer's fraud notification, a CRA must, within three days of the notification, provide the consumer with all of the disclosures required under 15 U.S.C. § 1681g. 15 U.S.C. § 1681c-1(a)(2), 1681c-1(b)(2). When a consumer requests that an "extended" fraud alert be placed on their files, the consumer is entitled to request two free disclosures under 15 U.S.C. § 1681g within the 12-month period following notification of a fraud alert. 15 U.S.C. § 1681c-1(b).

15. Thus, through immediate review of the details of when, and for what purpose, a consumer's private information has been disclosed to a third party, a consumer may better understand whether their identity has been stolen. And through semi-annual review of their consumer disclosures in the case of an "extended" alert, a consumer can periodically check to determine whether efforts to protect their

identity after potential fraud have not been successful. Thus, the FCRA presupposes that consumers subject to potential fraud should be permitted the immediate opportunity to investigate the issues themselves and ascertain the extent of any suspected fraud.

16. Plaintiff, individually and on behalf of those similarly situated, bring this lawsuit to challenge the actions of Defendant in the protection and safekeeping of the Plaintiff's and Class members' personal information.

17. Defendant failed to properly safeguard the information of Plaintiff and Class members, as required under 15 U.S.C. § 1681e(a).

### **GENERAL ALLEGATIONS**

18. On July 29, 2017, Equifax discovered that one or more of its servers, which contained Plaintiff's sensitive personal information, including Plaintiff's name, full Social Security number, birth date, address, and, upon belief, his driver's license number and possibly one or more of his credit cards, had been breached or "hacked" by a still unknown third party.

19. Upon belief, when Equifax discovered this breach, Equifax immediately began an internal investigation and contracted with an unidentified third-party cybersecurity firm to conduct a comprehensive forensic review to determine the scope of the hack including identifying the specific data impacted. As

of the filing of this Complaint, that investigation remains ongoing and has not yet been completed despite over six weeks elapsing since the initial breach.

20. On September 7, 2017, major news outlets began reporting about the July 29, 2017 incident. (See, e.g., *Massive Equifax Data Breach Could Impact Half of the U.S. Population*, Alyssa Newcomb, NBCNEWS, Sept. 7, 2018, available at: <https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686>).

21. For the Plaintiff and Class members, these news stories were the first time that they had been informed that their information secured by Equifax had been compromised six (6) weeks earlier, and they now live in constant fear that their information has been compromised.

22. Equifax's decision to wait six (6) weeks after the alleged data breach before informing all consumers of the same was willful, or at least negligent. Further, by depriving Plaintiff and Class members information about the breach in a timely manner, Equifax subjected each consumer to a concrete informational injury, as these consumers were deprived of their opportunity to meaningfully consider and address issues related to the potential fraud, as well as to avail themselves of the remedies available under the FCRA to prevent further dissemination of their private information.

23. Equifax has been subject to numerous allegations regarding data breaches in the past. (*See, e.g., A Brief History of Equifax Security Fails*, Thomas Fox-Brewster, FORBES, Sept. 8, 2017, available at: <https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#63dc4270677c>). In light of Equifax's continual failure to ensure the integrity of its file storage systems in light of known defects to the same, Equifax willfully, or at least negligently, failed to enact reasonable procedures to ensure that consumer reports would only be provided for a permissible purpose. By failing to establish reasonable procedures to safeguard individual consumer's private information, Equifax deprived millions of consumers from a benefit conferred on them by Congress, which, now lost, cannot be reclaimed.

24. The harm to Plaintiff and Class members was complete at the time the unauthorized breaches occurred, as the unauthorized disclosure and dissemination of private credit information causes harm in and of itself.

25. On September 7, 2017, Equifax began to offer consumers like the Plaintiff and Class members an allegedly dedicated secure website where consumers could determine if their information was compromised (<https://www.equifaxsecurity2017.com>) and offer consumers "free" credit monitoring through an Equifax product, TrustedID Premier (<https://www.equifaxsecurity2017.com/enroll/>), for one year.

26. However, under the guise of an effort to mitigate damages and to provide some assistance to the victims of its data breach, including Plaintiff and Class members, by allowing them free access to Defendant's TrustedID Premier service, the terms and conditions of that free service require that the victims, including Plaintiff and Class members, waive their right to bring or participate in a class action lawsuit and require them to submit to arbitration (<http://www.equifax.com/terms/>). This is another avenue to deprive the Plaintiff and Class members of the ability to avail themselves of the remedies available under federal law to obtain compensation for the data breach and prevent further dissemination of their private information.

### **CLASS ALLEGATIONS**

27. Plaintiff brings this action on behalf of a nationwide class of all similarly situated individuals ("Class"), defined as: "all persons in the United States for whom Equifax stored private, personal information that was released as a result of the data breach."

28. Excluded from the Class are: (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request

for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

29. Plaintiff does not know the size of the Class at this time because the information is exclusively in the possession of the Defendant, but Plaintiff believes that the potential number of Class members are so numerous that joinder would be impracticable. It has been reported that the Class could consist of over 100 million people. The number of Class members can be determined through discovery.

30. All members of the Class have been subject to and affected by a uniform course of conduct in that all Class members' personal information was compromised during the data breach. These are questions of law and fact common to the proposed Class that predominate over any individual questions. The questions common to all Class members include, but are not limited to:

- a. Whether Defendant had implemented reasonable procedures to ensure that all third parties who accessed Plaintiff's and Class members' private credit information did so for a permissible purpose;
- b. Whether Defendant failed to notify consumers of the data breach within a reasonable period of time;
- c. Whether Defendant failed to block the reporting of information on consumers' files that were the result of the data breach;
- d. Whether Plaintiff and Class members suffered damages as a result of Defendant's failure to comply with FCRA based on the improper dissemination of their credit information as a result of the data breach;

- e. Whether Plaintiff and Class members are entitled to statutory damages; and
- f. Whether Plaintiff and Class members are entitled to punitive damages.

31. Plaintiff's claims are typical of the class, as Plaintiff's personal information was compromised during the data breach. All claims are based on the same legal and factual issues.

32. Plaintiff will adequately represent the interests of the class and does not have an adverse interest to the class. If individual class members prosecuted separate actions it may create a risk of inconsistent or varying judgments that would establish incompatible standards of conduct. A class action is the superior method for the quick and efficient adjudication of this controversy. Plaintiff's counsel has experience litigation consumer class actions.

33. Further, under Fed. R. Civ. Pro. 23(a), Defendant acted on grounds generally applicable to the proposed Class, making appropriate final declaratory and injunctive relief with respect to the proposed Class as a whole.

**COUNT ONE: VIOLATION OF 15 U.S.C. §§ 1681, et al.**

34. Plaintiff restates all allegations set forth above and below as if fully rewritten herein.

35. This Count is brought on behalf of the nationwide Class.

36. Based upon Equifax's failure to have reasonable procedures in place, Plaintiff's private information was compromised, and neither the Plaintiff nor Class members received notice of the data breach, except through the media, approximately six (6) weeks after the breach occurred.

37. As a result of each and every willful violation of FCRA, Plaintiff and Class members are entitled to: actual damages, pursuant to 15 U.S.C. § 1681n(a)(1); statutory damages, pursuant to 15 U.S.C. § 1681n(a)(1); punitive damages, as this Court may allow, pursuant to 15 U.S.C. § 1681n(a)(2); and reasonable attorneys' fees and costs pursuant to 15 U.S.C. § 1681n(a)(3).

38. As a result of each and every negligent non-compliance of the FCRA, Plaintiff and Class members are also entitled to actual damages, pursuant to 15 U.S.C. § 1681o(a)(1); and reasonable attorney's fees and costs pursuant to 15 U.S.C. § 1681o(a)(2) from Defendant.

### **COUNT THREE: DECLARATORY JUDGMENT**

39. Plaintiff restates all allegations set forth above and below as if fully rewritten herein.

40. At all relevant times, there was in effect the Declaratory Judgment Act ("DJA"), 28 U.S.C. § 2201(a), which states, in relevant part:

In a case of actual controversy within its jurisdiction... any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested

party seeking such declaration, whether or not further relief is or could be sought. Any such declaration shall have the force and effect of a final judgment or decree and shall be reviewable as such.

28 U.S.C. § 2201(a).

41. Plaintiff and Class members seek an order declaring that the arbitration clause and class action waiver in the TrustedID Premier Terms of Use are invalid and do not apply to any claims they may have arising out of the data breach.

42. The controversy presented in this case is definite and concrete, and affects the adverse legal interests of the parties. As a result of the data breach and the release of Plaintiff's and Class members' private personal information, Plaintiff and Class members are at a great risk of having that personal information used by unauthorized individuals.

43. To safeguard against the unauthorized use of the personal information that was kept by Defendant, Plaintiff and Class members must obtain credit monitoring. The need for credit monitoring is urgent, as the information that Equifax failed to safeguard is extremely sensitive and can be used steal Plaintiff's and Class members' identities, which can lower their credit scores, cost money, and cause severe emotional distress. (*See Victims of Identity Theft, 2014*, Erika Harrell, Ph.D., U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS, (Sept. 2015), *available at*: <https://www.bjs.gov/content/pub/pdf/vit14.pdf> (stating that half of the victims of identity theft suffered losses of more than \$100, identity theft losses totaled more

than \$15.4 billion in 2014, and identity theft victims frequently experience “moderate or severe emotional distress as a result of the incident.”).

44. Defendant established a website that allows individuals to check to see if their personal information is at risk, and it allows individuals to enroll in a year of free credit monitoring through Defendant’s credit monitoring program, TrustedID Premier.

45. However, the “TrustedID Premier Terms of Use” include provisions that require enrollees to settle all disputes with Defendant—including Defendant’s failure to adequately safeguard Plaintiff’s and Class members’ private personal information—through binding, individual arbitration, “even if the facts and circumstances upon which the claims are based already occurred or existed.” (*See, TrustedID Premier Terms of Use, EQUIFAX, available at: <https://trustedidpremier.com/static/terms>*).

46. As such, Defendant is requiring all Class members to waive their right to participate in a class action for their claims arising out of the data breach, and to submit their individual claims to arbitration, before Defendant will assist those individuals with necessary credit monitoring to prevent the harm that Defendant has caused.

47. The only other option Class members have to protect themselves is to pay for credit monitoring on their own. For Class members who cannot afford to

purchase credit monitoring on their own, they are forced to either waive their right to participate in a class action, or forego any credit monitoring and face the risk of identity theft without any protection.

48. Further, many individuals have reported that even when inputting fake or incorrect information into Defendant's website, Defendant still informs those individuals that their personal information is part of the data breach, and that they should sign up for Defendant's credit monitoring, thereby waiving any right to participate in a class action.<sup>1</sup>

49. Moreover, if the individual does not cancel Defendant's credit monitoring program by calling Defendant, Defendant will begin charging those individuals for the credit monitoring after one year.<sup>2</sup> As a result, Defendant will profit off of those persons who were harmed by Defendant's failure to adequately safeguard Plaintiff's and Class members' personal information.

50. Therefore, enforcing the arbitration clause and class action waiver in the TrustedID Premier Terms of Use is unfair to Plaintiff and Class members,

---

<sup>1</sup> See *Why Some Are Recommending "Credit Freezes" in the Wake of the Gigantic Equifax Data Breach*, Tom McKay, Gizmodo, Sept. 9, 2017, available at: <http://gizmodo.com/why-some-are-recommending-credit-freezes-in-the-wake-1802924951>

<sup>2</sup> See *id.*

because the waivers are obtained through duress, cause harm to the Plaintiff and Class members, and are unconscionable.

51. There is an actual controversy between the parties of sufficient immediacy and reality to warrant the issuance of a declaratory judgment because Defendant is requiring Class members to (a) waive legal rights they have against Defendant in order to prevent additional harm with Defendant's credit monitoring, (b) pay for credit monitoring themselves, or (c) forego credit monitoring altogether.

52. Consequently, Plaintiff and Class members have been, and will continue to be, caused significant harm in that they must choose between waiving legal rights or risking additional identity theft. Plaintiff and Class members will continue to suffer harm if the Court were to deny their request for declaratory relief, as the harm of identity theft is ongoing.

53. If the Court were to deny Plaintiff's and Class members' request for declaratory relief, this controversy will continue to exist, as they must continue to pay for credit monitoring or risk additional identity theft, or waive legal rights against Defendant, and many Class members will continue to face this dilemma until this case is resolved.

54. There are no disputed legal and factual issues that the Court would have to resolve in granting Plaintiff's and Class members' request for declaratory relief, as this issue does not affect the merits of Plaintiff's and Class members' claims

against Defendant, and instead seeks to preserve the *status quo*—i.e., that Plaintiff and Class members have the right to pursue their claims against Defendant arising out of the data breach in Court as part of a class action lawsuit.

55. Based on the foregoing facts, the Court should declare the arbitration clause and class action waiver in the TrustedID Premier Terms of Use are invalid and do not apply to any claims they may have arising out of the data breach.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff DAVID CAPLAN, individually and on behalf of the Class, respectfully request the following relief against Defendant Equifax Information Services, LLC:

- A) For an award of actual damages against Defendant for all allegations contained in Count One;
- B) For an award of statutory damages pursuant to 15 U.S.C. § 1681n(a)(1) against Defendant for the allegations contained in Count One for each eligible Class member and the Plaintiff;
- C) For an award of punitive damages against Defendant for the allegations contained in Count One and as this Court may allow pursuant to 15 U.S.C. § 1681n(a)(2);
- D) For an award of the costs of litigation and reasonable attorneys' fees pursuant to 15 U.S.C. § 1681n(a)(3) and 15 U.S.C. § 1681(o)(1)(1) against Defendant for each incident of noncompliance of FCRA alleged in Count One;
- E) For an order declaring the arbitration clause and class action waiver in the TrustedID Premier Terms of Use invalid and inapplicable to the claims Plaintiff and the Class members may have arising out of the data breach;

- F) For a preliminary and permanent injunction prohibiting Equifax from continuing to bait and switch consumers into signing a class action waiver and arbitration agreement that would apply to any claims they may have arising out of the data breach; and
- G) For all other relief this Court may deem just and proper.

Respectfully Submitted,



Andrew B. Sacks (PA #41390)

*asacks@sackslaw.com*

John K. Weston (PA #26314)

*jweston@sackslaw.com*

Jeremy E. Abay (PA #316730)

*jabay@sackslaw.com*

SACKS WESTON DIAMOND, LLC

1845 Walnut Street, Suite 1600

Philadelphia, Pennsylvania 19103

T: (215) 925-8200

F: (267) 639-5422

Thomas A. Zimmerman, Jr.

*tom@attorneyzim.com*

ZIMMERMAN LAW OFFICES, P.C.

77 W. Washington Street, Suite 1220

Chicago, Illinois 60602

T: (312) 440-0020 telephone

F: (312) 440-4180 facsimile

*Pro Hac Vice Application to Be Submitted*

Robert A. Clifford

*rac@cliffordlaw.com*

Shannon M. McNulty

*smm@cliffordlaw.com*

CLIFFORD LAW OFFICES, P.C.  
120 N. LaSalle Street, Suite 3100  
Chicago, Illinois 60602  
T: (312) 899-9090  
F: (312) 899-9090

Marc E. Dann  
Brian D. Flick  
*notices@dannlaw.com*  
DANNLAW  
P.O. Box 6031040  
Cleveland, OH 44103  
T: (216) 373-0539  
F: (216) 373-0536  
*Pro Hac Vice Application to Be Submitted*

David H. Krieger  
*dkrieger@hainesandkrieger.com*  
HAINES & KRIEGER, LLC  
8985 S. Eastern Avenue, Suite 350  
Henderson, NV 89123  
T: (702) 880-5554  
F: (702) 385-5518  
*Pro Hac Vice Application to Be Submitted*

Matthew I. Knepper  
*matthew.knepper@knepperclark.com*  
Miles N. Clark  
*miles.clark@knepperclark.com*  
KNEPPER & CLARK LLC  
10040 W. Cheyenne Ave., Suite 170-109  
Las Vegas, NV 89129  
T: (702) 825-6060  
F: (702) 447-8048  
*Pro Hac Vice Application to Be Submitted*

Sean N. Payne  
*seanpayne@spaynelaw.com*  
PAYNE LAW FIRM LLC  
9550 S. Eastern Ave. Suite 253-A213

Las Vegas, NV 89123

T: 702-952-2733

F: 702-462-7227

*Pro Hac Vice Application to Be Submitted*

*Counsel for the Plaintiff and the Class*

**JURY DEMAND**

Plaintiff hereby requests a trial by jury on all issues so triable.

A handwritten signature in dark ink, appearing to read 'Andrew B. Sacks', is written over a horizontal line.

Andrew B. Sacks

*Counsel for Plaintiff and the Class*